U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON

| | |
|---|---|
| CASEY DEVINE, individually and on behalf of all others similarly situated,<br><br>Plaintiff,<br><br>vs.<br><br>PREMERA BLUE CROSS, a Washington corporation,<br><br>Defendant. | NO.<br><br>**CLASS ACTION COMPLAINT**<br><br>**Demand for Jury Trial** |

Plaintiff Casey Devine ("Devine" or "Plaintiff") alleges the following, upon personal knowledge with respect to himself, and on information and belief derived from, among other things, investigation of counsel and review of public documents, as to all other matters:

## I. NATURE OF THE CASE

1. This is a class action on behalf of the millions of customers of Premera Blue Cross whose personal, health, and financial information were accessed by one or more criminal actors in a consumer data security breach. Plaintiff seeks relief under Washington law on behalf of all consumers in the United States who had their personal, health, and financial information compromised as a result of the breach. Plaintiff also seeks relief under Washington law on



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

behalf of the millions of customers of Premera in Washington who had their personal, health, and financial information compromised.

2. Defendant Premera Blue Cross is one of the largest health insurance companies in the Pacific Northwest. In Washington and Alaska alone, there are nearly 2 million individuals currently insured by Premera Blue Cross. Premera Blue Cross is a major provider to, among others, Amazon.com Inc., Microsoft Corp., and Starbucks Corp. Unsurprisingly, Premera Blue Cross maintains a massive amount of personal, health, and financial information on its past and current insureds. It therefore has a duty to take all reasonable measures to protect this information and safeguard it from theft.

3. On March 17, 2015, Premera announced that hackers had breached its systems and compromised personal, health, and financial information of up to 11 million Premera health insurance plan customers, former customers, and members of other Blue Cross Blue Shield plan who sought treatment in Washington and Alaska.

4. Premera has yet to individually notify all affected individuals about what specific data of theirs has been compromised, saying only that it anticipates to inform all affected individuals by April 20, 2015. It has nevertheless advised that the compromised data included name, address, email address, telephone number, date of birth, Social Security number, member identification number, medical claims information and in some cases, bank account information. What is worse, the cyber security systems of Premera Blue Cross were breached just weeks after federal auditors explicitly warned Premera that its security systems were inadequate and could be exploited. This theft is the result of Defendant's failure to implement cyber security measures commensurate with the duties it undertook by storing vast quantities of sensitive customer data.

5. Further, and to compound the harm caused to its customers, Premera Blue Cross knew about the breach for over six weeks before it publicly disclosed the incident. Indeed,



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

Premera Blue Cross has acknowledged that it first learned that its system was compromised on January 29, 2015. It did nothing to warn its customers for over six weeks.

6. This breach occurred because of Premera's failure to take reasonable measures to ensure its data systems were adequate to protect the sensitive personal data of its customers and former customers. Among other things, Premera failed to implement data security measures designed to prevent this attack despite repeated warnings to the healthcare industry and Premera about the risks of such cyber attacks, failed to employ security protocols to detect the unauthorized network activity, failed to maintain basic security measures such as complex data encryption so that if data were accessed or stolen it would be unreadable, failed to disclose to its customers the material facts that it did not have adequate computer systems and data security practices to safeguard customers' personal data, and failed to provide immediate and accurate notice of the data breach to its customers. These failures have injured Plaintiff and the Class.

7. Devine was a member of Blue Cross Blue Sheild of Minnesota and received medical treatment in Washington State. Devine's insurance was provided by his former employer, Travlers Indemnity Corporation and covered Devine and his daughter. Like millions of other Premera customers, Plaintiff's personal, health, and financial information has been compromised. In its statement about the matter, Premera stated that "This incident also affected members of other Blue Cross Blue Shield plans who sought treatment in Washington or Alaska."[1]

8. Because of Defendants' negligence, some 11 million customers had their personal, health, and financial information, including name, address, email address, telephone number, date of birth, Social Security number, member identification number, medical claims information and in some cases, bank account information, compromised by criminal hackers.

[1] http://www.premeraupdate.com/ (last visited Apr. 7, 2015).

TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

9. The information obtained as a result of the conduct complained of herein is a treasure trove for identity thieves who use it to gain access to every aspect of a victim's life, or worse, to create a new life using the victim's identity for years to come.

## II. JURISDICTION AND VENUE

10. Jurisdiction is proper in this Court pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because members of the proposed Plaintiff Class are citizens of states different from Defendant's home state, and the aggregate amount in controversy exceeds in $5,000,000 exclusive of interests and costs.

11. This Court has personal jurisdiction over Premera because Premera is licensed to do business in Washington, regularly conducts business in Washington, and has minimum contacts with Washington.

12. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a) because Premera regularly conducts business and resides in this district, a substantial part of the events or omissions giving rise to these claims occurred in this district, and Premera has caused harm to class members residing in this district.

## III. PARTIES

13. Devine is a citizen of Spokane, Washington, and maintained health insurance with Blue Cross Blue Shield of Minnesota and received treatment in Washington using his Blue Cross Blue Shield insurance. Upon information and belief and Premera's statements to its customers as a whole, Devine had his personal, health, and possibly his financial information compromised a result of the Premera data breach.

14. Premera is a Washington corporation registered with the Washington Secretary of State to do business in Washington. Premera's corporate headquarters are located at 7001 220th Street SW, Mountlake Terrace, Washington, 98043. Premera also maintains operations in Seattle and Spokane, Washington.



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

15. Premera provides healthcare benefits in Alaska as Premera Blue Cross Blue Shield of Alaska. It has registered with the Alaska Secretary of State to do business in Alaska. Premera and Premera Blue Cross Blue Shield of Alaska are independent licensees of the Blue Cross Blue Shield Association.

16. Premera also maintains several affiliates that are not licensees of the Blue Cross Blue Shield Association. These affiliates include LifeWise Health Plan of Oregon; LifeWise Health Plan of Washington; LifeWise Assurance Company; Connexion Insurance Solutions, Inc.; and Vivacity. In total, Premera's affiliates maintain 1.9 million current members in Washington, Alaska, and Oregon.

17. Premera, Premera Blue Cross Blue Shield of Alaska, and its affiliates are collectively referred to as "Premera" in this Complaint.

## IV. FACTUAL BACKGROUND

18. Premera is one the largest health insurance providers in the Pacific Northwest. There are over 6 million current or former Premera insureds in Washington alone.[2]

19. Premera states its Mission is to "provide peace of mind to our customers about their healthcare."[3] To that end, Premera provides each of its customers with a Notice of Privacy Practices.[4] It also dedicates a section of its website to explain its privacy and data collection policies.[5]

20. Premera promises its customers that it is "committed to maintaining the confidentiality of your medical and financial information," which necessarily includes the very data accessed through the breach of Premera's systems. Premera assures its customers that it has secured its "electronic systems against unauthorized access," and it acknowledges that

---

[2] *See* http://www.seattletimes.com/business/technology/premera-hit-by-cyberattack-11m-customers-may-be-affected/ (last visited Apr. 2, 2015)

[3] https://www.premera.com/wa/visitor/about-premera/fact-sheet/ (last visited Apr. 2, 2015).

[4] *See* Notice of Privacy Practices, *available at* https://www.premera.com/documents/000160.pdf (last visited Mar. 23, 2015).

[5] *See* https://www.premera.com/wa/visitor/privacy-policy/ (last visited Mar. 22, 2015). The privacy section of Premera's website is substantially similar to the printed Notice of Privacy Practices provided to each Premera customer.

TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

"[u]nder both the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Gramm-Leach-Bailey Act, Premera Blue Cross must take measures to protect the privacy of your personal information." Further, Premera warrants that it will "protect the privacy of your information even if you no longer maintain coverage through us."

21. Premera further states that it is required by law to "notify [customers] following a breach of . . . unsecured personal information."

22. On or about May 5, 2014, hackers obtained access to Premera's computer network. Over the course of the following eight months, they compromised as many as 11 million records of current and former Premera customers and employees, as well as Blue Cross Blue Shield customers who received medical treatment in Washington or Alaska. For each affected customer, hackers were able to access the customer's name, date of birth, email address, address, telephone number, Social Security number, member identification number, bank account information, and claims information, including clinical data.

23. Premera did not disclose that hackers had gained access to its system until January 29, 2015, nine months after the hackers had first entered Premera's systems.

24. Even after learning of the breach, Premera failed to timely notify its customers or the public of the breach, waiting until March 17, 2015 to disclose the breach, over six weeks after Premera learned of the unauthorized access to its systems.

25. On March 17, 2015, Premera disclosed publicly that hackers had obtained access to its computer systems and compromised the personal, financial, and health information of 11 million current and former customers and employees. Customer records as far back as 2002 were affected by the breach.

26. Premera President Jeffrey Roe issued a statement accompanying the company's public disclosure. In it, he confirmed that attackers "gain[ed] unauthorized access to [Premera's] Information Technology (IT) systems." Mr. Roe's statement further confirmed that the compromised data included "member name, date of birth, email address, address, telephone



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

number, Social Security number, member identification numbers, bank account information, and claims information, including clinical information."[6]

27. Upon information and belief, hackers were able to access customers' health and financial information because Premera did not maintain adequate access controls for its computer network or store such information on separate databases.

28. Premera also failed to maintain adequate network security to prevent and/or monitor unauthorized access to its computer networks, including those on which private customer data was stored.

29. Premera was explicitly warned by the federal government that its cyber security systems were vulnerable before the breach occurred in May 2014. On April 18, 2014, the Office of Personnel Management delivered the results of an audit it performed on Premera's computer systems. The audit identified ten areas in which Premera's systems were inadequate and vulnerable to attack.[7]

30. Specifically, the audit found that Premera was not timely implementing critical security patches and other software updates. The audit warned, "Failure to promptly install important updates increases the risk that vulnerabilities will not be remediated and sensitive data could be breached."[8]

31. Specifically, the audit found that Premera failed to implement software patches, including critical patches, service packs, and hot fixes, in a timely manner and lacked a methodology for ensuring it did not use unsupported or otherwise out-of-date software.

---

[6] *Id.*

[7] *See* Feds Warned Premera About Security Flaws Before Breach, Seattle Times, Mike Baker, Mar. 18, 2015, *available at* http://www.seattletimes.com/business/local-business/feds-warned-premera-about-security-flaws-before-breach/ (last visited Mar. 22, 2015).

[8] U.S. Office of Personnel Management, Office of the Inspector General, Office of Audits, Audit of Information Systems General and Application Controls at Premera Blue Cross 7 (Nov. 28, 2014), https://s3.amazonaws.com/s3.documentcloud.org/documents/1688453/opm-audit.pdf. The Final Audit Report was delivered to Premera on November 28, 2014, but the audit's initial findings were delivered to Premera in April 2014. Premera then had an opportunity to respond before the audit findings became final.



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

32. Also, one or more of Premera's servers contained software applications that were no longer supported by the software's vendors and had known security vulnerabilities.

33. In addition, Premera's servers were insecurely configured, which rendered them more vulnerable to hacking.[9]

34. Three weeks after Premera received this audit, its system was compromised.

35. In its public disclosure on March 17, 2015, Premera promised that it would notify customers of the breach by letter and that it would not complete this notification process until April 20, 2015, almost three months after Premera first learned of the data breach.

36. Unlike some Premera customers, Devine has received no communication from Premera concerning the data breach. Devine has only received communication from Travelers and Blue Cross Blue Shield of Minnesota concerning the data breach.

37. Because of the wealth of information stored on their systems healthcare providers, such as Premera, are aware that they are, and will be, a frequent target of attacks on data security.

38. According to a report issued by the credit reporting company Experian, "[t]he healthcare industry, by far, will be the most susceptible to publicly disclosed and widely scrutinized data breaches."[10]

39. The New York Times reports that "[t]he threat of a hacking is particularly acute in the health care and financial services industries, where companies routinely keep the most sensitive personal information about their customers on large databases."[11]

40. In fact, the type of data stored by healthcare providers, and stolen as part of the Premera data breach, is far more valuable to identity thieves than credit card or other personally identifiable information stolen from retailers or other companies that store customer

---

[9] *Id.* at 8.
[10] http://www.experian.com/data-breach/data-breach-industry-forecast.html (last visited Apr. 2, 2015)
[11] *See* Reed Abelson & Matthew Goldstein, Millions of Anthem Customers Targeted in Cyberattack, N.Y. TIMES (Feb. 10, 2015), http://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

information. This is because a credit card can be easily cancelled or replaced. A social security number cannot.

41. This information allows thieves to open many financial/banking accounts in victims' names, and in some cases to file fake tax returns in their names – a common fraud.

42. An April 2014 notice from the Federal Bureau of Investigation to health care providers warned companies, including Premera, about the inadequacies of their systems, given the threats that exist. The notice stated: "[t]he healthcare industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely." FBI Cyber Division, Private Industry Notification, PIN # 140408-010.

43. In August, 2014 after a data breach at Community Health, the FBI again warned those in the healthcare industry about the need for increased data protection, saying that it had "observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[12]

44. The Federal Trade Commission describes identity theft as "when someone steals your personal information and uses it without your permission." Going on to describe it as "a serious crime that can wreak havoc with your finances, credit history, and reputation — and can take time, money, and patience to resolve."[13]

45. According to the FTC "Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. An identity thief can file a tax refund in your name and get your refund. In some extreme cases, a thief might even give your name to the police during an arrest."[14]

---

[12] *See* http://www.politico.com/morningcybersecurity/0814/morningcybersecurity15083.html (Last visited Apr. 2, 2015).
[13] *See* http://www.consumer.ftc.gov/features/feature-0014-identity-theft (Last visited Apr. 2, 2015).
[14] http://www.consumer.ftc.gov/articles/0271-signs-identity-theft.



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

46. On May 10, 2006, President Bush established the President's Task Force on Identity Theft ("Task Force"), "recognizing the heavy financial and emotional toll that identity theft exacts from its victims, and the severe burden it places on the economy."

47. The Task Force's report recognizes that "individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration."

48. According to the Indiana Attorney General's office "The risk of identity theft is a lot like germs – you can be aware and take precautions but you cannot avoid the risk completely. You can only be smart about the behaviors you use and educate those around you." You cannot, however, control the cavalier actions of your insurance carrier.

49. As the Minnesota Attorney General has pointed out, in the case of identity theft "it may take a few months, but eventually you'll start getting calls from creditors demanding payment for charges that you never made. A strange bank may call you about an overdrawn account in your name – an account you never opened. Identity theft takes months for you to detect, and sometimes years or longer to unravel."

50. On March 20, 2015, following news of the Premera breach, Sen. Patty Murray, a ranking member of the Senate Health, Education, Labor and Pensions Committee, demanded answers to questions related to the breach[15] and both Murray and Washington State Insurance Commissioner Mike Kreidler launched investigations into Premera.[16]

[15] http://www.seattletimes.com/business/murray-letter-demands-answers-from-premera-on-cyberattack/ (last visited Apr. 2, 2015).
[16] http://www.seattletimes.com/seattle-news/premera-negligent-in-data-breach-5-lawsuits-claim/ (last visited Apr. 2, 2015).



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

51. Murray was quoted saying she had "serious[] concern[s] about the pace of notification, as well as how impacted families and businesses are being informed and assisted."[17]

52. The unauthorized disclosure of Social Security Numbers can be particularly damaging, because Social Security Numbers cannot easily be replaced. In order to obtain a new number, a person must prove, among other things, that he or she continues to be disadvantaged by the misuse. Thus, no new number can be obtained until after the damage has been done. Furthermore, as the Social Security Administration ("SSA") warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.

53. If you receive a new Social Security Number, you should not be able to use the old number anymore.

54. For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more it difficult for you to get credit.[18]

55. Because of Premera's failure to protect its customers' private information, Plaintiff and the Class now face years of looking over their financial shoulder, monitoring their credit reports, and paying for identity theft protection.

---

[17] http://www.seattletimes.com/seattle-news/premera-negligent-in-data-breach-5-lawsuits-claim/ (last visited Apr. 2, 2015).

[18] *See* SSA, Identity Theft and Your Social Security Number, SSA Publication No. 05-10064 (Dec. 2013), available at http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Feb. 11, 2015).



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

## V. CLASS ACTION ALLEGATIONS

56. Plaintiff brings this action pursuant to Washington law on behalf of himself and all other persons similarly situated pursuant to Fed. R. Civ. P. 23 defined as follows:

> All persons in the United States whose personal, health, and/or financial information was stored on the Premera system, and who have had their personal, health, and/or financial information exposed during the security breach, announced on March 17, 2015 and were or may be damaged ("Nationwide Class").

Excluded from the class are Defendant, any parent, subsidiary or affiliate of Defendant, legal representatives, successors, or assigns of Defendant and any justice, judge or magistrate judge of the United States who may hear the case, and all persons related to any such judicial officer as defined in 28 U.S.C. §455(B).

57. Plaintiff also brings this action pursuant to Washington law on behalf of himself and a subclass of all other persons similarly situated pursuant to Fed. R. Civ. P. 23 defined as follows:

> All persons in Washington whose personal, health, and/or financial information was stored on the Premera system, and who have had their personal, health, and/or financial information exposed during the security breach, announced on March 17 2015 and were or may be damaged ("Washington Class").

Excluded from the Class are Defendant; any parent, subsidiary, or affiliate of Defendant or any employees, officers, or directors of Defendant; legal representatives, successors, or assigns of Defendant; and any justice, judge or magistrate judge of the United States who may hear the case, and all persons related to any such judicial officer, as defined in 28 U.S.C. § 455(b).

58. **Numerosity.** The Class members are so numerous and dispersed nationwide that joinder of all members is impracticable. Upon information and belief, the Class members number in the millions. The exact number of Class members is unknown, but can be determined from Defendant's computerized and other records. Plaintiff reasonably estimates and believes that there are millions of persons in the Class.



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

59. **Commonality.** There are numerous and substantial questions of law and fact that are common to all members of the Class, which predominate over any question affecting only individual Class members. The members of the Class were and continue to be subjected to the same practices of the Defendant. The common questions and issues raised by Plaintiff's claims include:

a. whether Defendant acted negligently in failing to properly safeguard Class members' financial and personal data;

b. whether Defendant's conduct constituted bailment;

c. whether Defendant violated industry standards concerning the handling and storage of Class members' financial and personal data;

d. whether Defendant failed to notify Class members of the security breach as soon as practical after the breach was discovered;

e. whether Defendant engaged in unfair practices by failing to properly safeguard customers' financial and personal data;

f. whether Defendant violated the Washington Consumer Protection Act RCW 19.86.010 et seq.;

g. whether Defendants violated RCW 19.255.010;.

h. whether Plaintiff and the Class have been damaged, and, if so, what types of damages flowed from Defendant's unlawful conduct; and

i. the appropriate measure of damages and remedies against Defendant, and the nature and extent of any other remedies, and injunctive relief, to which Plaintiff and the Class are entitled.

60. **Typicality.** Plaintiff's claims are typical of the claims of all of the other members of the Class because his claims are based on the same legal and remedial theories as the claims of the Class and arise from the same course of conduct by Defendant.



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

61. **Adequacy.** Plaintiff will fairly and adequately protect the interests of all members of the Class in the prosecution of this Action and in the administration of all matters relating to the claims stated herein. Plaintiff is similarly situated with, and has suffered similar injuries as, the members of the Class he seeks to represent. Plaintiff has retained counsel experienced in handling class action lawsuits. Neither Plaintiff nor his counsel have any interest that might cause them not to vigorously pursue this action.

62. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of the controversy since individual joinder of the Class members is impracticable. Even if individual Class members were able to afford individual litigation, it would be unduly burdensome to the Courts in which the individual litigation would proceed. Defendants have subjected the Class to the same violations as referenced herein. Accordingly, class certification is appropriate under Rule 23 because common issues of law and fact regarding Defendant's uniform violations predominate over individual issues, and class certification is a superior method of resolving these claims. No unusual difficulties are likely to be encountered in the management of this action as a class action. Defendant acted and continue to act in a manner that is generally applicable to all members of the Class, making final injunctive relief appropriate.

## VI. NEGLIGENCE

### (ON BEHALF OF THE NATIONWIDE CLASS, AND WASHINGTON SUBCLASS, PURSUANT TO WASHINGTON LAW)

63. Plaintiff fully incorporates by reference herein all of the above paragraphs, as though fully set forth herein.

64. Premera owed a duty to Plaintiff and members of the Class to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their personal, health, and financial information in its possession from being compromised. This duty included, among other things, designing, maintaining, and testing Premera's security systems to



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

ensure that Plaintiff's and Class members' personal, health, and financial information in Premera's possession was adequately secured and protected. Premera further owed a duty to Plaintiff and Class members to implement processes that would detect a breach of its security system in a timely manner and to timely act upon warnings and alerts.

65. Premera owed a duty, as articulated in Premera's Privacy Policies, to protect its customers' sensitive financial, health, and personal information.

66. Premera owed a duty to timely disclose the material fact that Premera's computer systems and data security practices were inadequate to safeguard customers' personal and financial data from theft.

67. Premera breached these duties by the conduct alleged in the Complaint by, including without limitation, (a) failing to protect its customers' personal, financial, and health information; (b) failing to maintain adequate computer systems and data security practices to safeguard customers' personal, health, and financial information; (c) failing to disclose the material fact that Premera's computer systems and data security practices were inadequate to safeguard customers' personal and financial data from theft; and (d) failing to disclose in a timely and accurate manner to Plaintiff and members of the Class the material fact of the Premera data breach.

68. The conduct alleged in the Complaint caused Plaintiff and Class members to be exposed to fraud and be harmed. The injuries suffered by the Plaintiff and the proposed Class as a direct result of the Premera data breach include: theft of their personal and financial information; costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts; costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

stress, nuisance and annoyance of dealing with all issues resulting from the Premera data breach; the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their personal and financial information being accessible by hackers; damages to and diminution in value of their personal and financial information entrusted to Premera for the sole purpose of obtaining health insurance from Premera and with the mutual understanding that Premera would safeguard Plaintiff's and Class members' data against theft and not allow access and misuse of their data by others; money paid to Premera for health insurance during the period of the Premera data breach in that Plaintiff and Class members would not have obtained insurance from Premera had Premera disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' financial and personal information and had Premera provided timely and accurate notice of the Premera data breach; overpayments paid to Premera for health insurance purchased during the Premera data breach in that a portion of the price for insurance paid by Plaintiff and the Class to Premera was for the costs of Premera providing reasonable and adequate safeguards and security measures to protect customers' financial and personal data, which Premera did not do, and as a result, Plaintiff and members of the Class did not receive what they paid for and were overcharged by Premera; and continued risk to their financial and personal information, which remains in the possession of Premera and which is subject to further breaches so long as Premera fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' data in its possession.

## VII. BREACH OF IMPLIED CONTRACT

## (ON BEHALF OF THE NATIONWIDE CLASS, AND WASHINGTON SUBCLASS, PURSUANT TO WASHINGTON LAW)

69. Plaintiff incorporates by reference those paragraphs set out above as if fully set forth herein.

70. When Plaintiff and members of the Class provided their financial, health, and personal information to Premera in order to purchase health insurance from Premera, Plaintiff



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

and members of the Class entered into implied contracts with Premera pursuant to which Premera agreed to safeguard and protect such information and to timely and accurately and individually notify Plaintiff and Class members that their data had been breached and compromised.

71. Plaintiff and Class members would not have provided and entrusted their financial, health, and personal information to Premera in order to purchase health insurance from Premera in the absence of the implied contract between them and Premera.

72. Plaintiff and members of the Class fully performed their obligations under the implied contracts with Premera.

73. Premera breached the implied contracts it made with Plaintiff and Class members by failing to safeguard and protect the personal, health, and financial information of Plaintiff and members of the Class and by failing to provide timely and accurate notice to them that their personal and financial information was compromised in and as a result of Premera data breach.

## VIII. BREACH OF CONTRACT

**(ON BEHALF OF THE NATIONWIDE CLASS, AND WASHINGTON SUBCLASS, PURSUANT TO WASHINGTON LAW)**

74. Plaintiff incorporates by reference those paragraphs set out above as if fully set forth herein.

75. Premera has a contractual obligation to maintain the security of its customers' personal, health, and financial information, which Premera itself recognizes in its Notice of Privacy Practices.

76. Premera promises its customers that it is "committed to maintaining the confidentiality of your medical and financial information," which necessarily includes the very data accessed through the breach of Premera's systems. Premera assures its customers that it has secured its "electronic systems against unauthorized access," and it acknowledges that "[u]nder both the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

the Gramm-Leach-Bailey Act, Premera Blue Cross must take measures to protect the privacy of your personal information." Further, Premera warrants that it will "protect the privacy of your information even if you no longer maintain coverage through us."

77. Premera further states that it is required by law to "notify [customers] following a breach of . . . unsecured personal information."

78. Premera breached these contractual obligations by failing to safeguard and protect the personal, health, and financial information of Plaintiff and members of the Class and by failing to provide timely and accurate notice to them that their personal and financial information was compromised in and as a result of Premera data breach.

79. The losses and damages sustained by Plaintiff and Class members as described herein were the direct and proximate result of Premera's breaches of the contracts between Premera and Plaintiff and members of the Class.

## IX. BAILMENT

## (ON BEHALF OF THE NATIONWIDE CLASS, AND WASHINGTON SUBCLASS, PURSUANT TO WASHINGTON LAW)

80. Plaintiff fully incorporates by reference herein all of the above paragraphs, as though fully set forth herein

81. Plaintiff and Class members delivered and entrusted their personal, health, and financial information to Premera for the sole purpose of receiving services from Premera.

82. In delivering their personal, health, and financial information to Premera, Plaintiff and Class members intended and understood that Premera would adequately safeguard their personal, health, and financial information.

83. Premera accepted possession of Plaintiff's and Class members' personal, health, and financial information. By accepting possession, Premera understood that Plaintiff and Class members expected Premera to adequately safeguard their personal and financial information. Accordingly, a bailment was established for the mutual benefit of the parties.



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

84. During the bailment, Premera owed a duty to Plaintiff and Class members to exercise reasonable care, diligence and prudence in protecting their personal, health, and financial information.

85. Premera breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiff's and Class members' personal, health, and financial information, resulting in the unlawful and unauthorized access to and misuse of such information.

86. Premera further breached its duty to safeguard Plaintiff's and Class members' personal, health, and financial information by failing to timely and accurately notify them individually that their information had been breached and compromised.

87. As a direct and proximate result of Premera's breach of its duty, Plaintiff and Class members suffered consequential damages that were reasonably foreseeable to Premera, including but not limited to the damages set forth above.

## X. UNJUST ENRICHMENT

## (ON BEHALF OF THE NATIONWIDE CLASS, AND WASHINGTON SUBCLASS, PURSUANT TO WASHINGTON LAW)

88. Plaintiff fully incorporates by reference herein all of the above paragraphs, as though fully set forth herein

89. Plaintiff and Class members conferred a monetary benefit on Premera in the form of monies paid for the purchase of health services from Premera during the period of the data breach.

90. Premera appreciates or has knowledge of the benefits conferred directly upon it by Plaintiff and members of the Class.

91. The monies paid for the purchase of health services by Plaintiff and members of the Class to Premera during the period of the data breach were supposed to be used by Premera, in part, to pay for the administrative and other costs of providing reasonable data security and protection to Plaintiff and members of the Class.



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

92. Premera failed to provide reasonable security, safeguards and protection to the personal, health, and financial information of Plaintiff and Class members and as a result, Plaintiff and Class members overpaid Premera for the services purchased.

93. Under principles of equity and good conscience, Premera should not be permitted to retain the money belonging to Plaintiff and members of the Class, because Premera failed to provide adequate safeguards and security measures to protect Plaintiff's and Class members' personal, health, and financial information that they paid for but did not receive.

94. Plaintiff and the Class have conferred directly upon Premera an economic benefit in the nature of monies received and profits resulting from sales and unlawful overcharges to the economic detriment of Plaintiff and the Class members.

95. The economic benefit, including the monies paid and the overcharges and profits derived by Premera and paid by Plaintiff and members of the Class, is a direct and proximate result of Premera's unlawful practices as set forth in this Complaint.

96. The financial benefits derived by Premera rightfully belong to Plaintiff and members of the Class.

97. A constructive trust should be imposed upon all unlawful or inequitable sums received by Premera traceable to Plaintiff and the Class.

98. Plaintiff and the Class have no adequate remedy at law.

## XI. FAILURE TO TIMELY DISCLOSE BREACH UNDER RCW 19.255.010

## (ON BEHALF OF THE WASHINGTON SUBCLASS)

99. Plaintiff fully incorporates by reference herein all of the above paragraphs, as though fully set forth herein.

100. Premera is a business conducting business in Washington and owns or licenses computerized data that includes personal information, as defined under RCW 19.255.010.



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

101. On or around May 5, 2014, Premera's computer system storing personal and financial information was breached, and unauthorized individuals gained access to the information.

102. Premera knew or should have known that the breach occurred, but due to its own negligent monitoring of its information systems, it did not discover the breach until January 29, 2015.

103. Premera then failed to notify the persons whose data was breached until May 17, 2015.

104. Premera's failure to detect and disclose the breach constituted an unreasonable delay.

105. As a direct and proximate result of Premera's failure to provide reasonably prompt disclosure, Plaintiff and the Class have suffered damages.

## XII. VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT RCW 19.86.010 *ET SEQ.*

**(ON BEHALF OF THE WASHINGTON SUBCLASS)**

106. Plaintiff realleges and incorporates by reference the allegations contained in the preceding paragraphs.

107. The conduct of Defendant as set forth herein constitutes unfair or deceptive acts or practices, including, but not limited to accepting and storing Plaintiff's' and the Class members' personal and financial information but failing to take reasonable steps to protect it. In violation of industry standards and best practices, Premera also violated consumer expectations to safeguard personal and financial information and failed to tell consumers that it did not have reasonable and best practices, safeguards, and data security in place.

108. Premera also violated the Washington Consumer Protection Act by failing to immediately notify Plaintiff and the Class of the data breach. If Plaintiff and the Class had been



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

notified in an appropriate fashion, they could have taken precautions to better safeguard their personal and financial information.

109. Defendant's actions as set forth above occurred in the conduct of trade or commerce.

110. To establish that an act is a "consumer" transaction it must be likely that "additional plaintiffs have been or will be injured in exactly the same fashion." *Hangman Ridge Training Stables, Inc. v. Safeco Title Ins. Co.*, 105 Wn.2d 778, 790 (1986).

111. Plaintiff was injured exactly the same way as millions of other Premera customers.

112. In a consumer transaction, the following factors determine whether the transaction "impacts the public interest":

> Were the alleged acts committed in the course of defendant's business? (2) Are the acts part of a pattern or generalized course of conduct? (3) Were repeated acts committed prior to the act involving plaintiff? (4) Is there a real and substantial potential for repetition of defendant's conduct after the act involving plaintiff? (5) If the act complained of involved a single transaction, were many consumers affected or likely to be affected by it? *Id.*

113. Defendant conducted the practices alleged herein in the course of its business pursuant to standardized practices that it engaged in both before and after the Plaintiff in this case was harmed, and many consumers were affected.

114. As a direct and proximate result of Target's negligence and misconduct described in this complaint, Plaintiff and the Class were injured in fact by: (a) (a) fraudulent charges; (b) theft of their personal and financial information; (c) costs associated with the detection and prevention of identity theft; (d) costs associated with the detection and prevention of unauthorized use of their financial accounts; (e) costs associated with being unable to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts; and (f) costs associated with the loss of productivity from taking



TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

time to ameliorate the actual and future consequences of the data breach, all of which have an ascertainable monetary value to be proven at trial.

115. Defendant's conduct proximately caused Plaintiff's and the Class's injuries.

116. Defendant is liable to Plaintiff and the Class for damages in amounts to be proven at trial, including attorneys' fees, costs, and treble damages.

## XIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests the following relief:

A. That the Court certify this case as a class action and appoint the named Plaintiff to be Class representatives and their counsel to be Class counsel;

B. That the Court award Plaintiff appropriate relief, to include actual and statutory damages, disgorgement, and restitution;

C. That the Court award Plaintiff preliminary or other equitable or declaratory relief as may be appropriate by way of applicable state or federal law;

D. That the Court enter such additional orders or judgments as may be necessary to prevent these practices and to restore to any person in interest any money or property which may have been acquired by means of the violations;

E. That the Court impose punitive damages under any provision of law under which punitive damages may be imposed;

F. That the Court award Plaintiff such other, favorable relief as may be available and appropriate under law or at equity;

G. That the Court award costs and reasonable attorneys' fees; and

H. That the Court enter such other and further relief as the Court may deem just and proper.

## XIV. JURY TRIAL DEMANDED

Plaintiff requests a trial to resolve all issues so triable.

TERRELL MARSHALL DAUDT & WILLIE PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.350.3528
www.tmdwlaw.com

RESPECTFULLY SUBMITTED AND DATED this 7th day of April, 2015.

TERRELL MARSHALL DAUDT & WILLIE PLLC

By: /s/ Beth E. Terrell, WSBA #26759
Beth E. Terrell, WSBA #26759
Email: bterrell@tmdwlaw.com
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
Telephone: (206) 816-6603
Facsimile: (206) 350-3528

Ariana J. Tadler
Email: atadler@milberg.com
Andrei V. Rado
Email: arado@milberg.com
John Seredynski
Email: jseredynski@milberg.com
Adam Bobkin
Email: abobkin@milberg.com
MILBERG LLP
One Pennsylvania Plaza, 49th Floor
New York, New York 10119
Telephone: (212) 594-5300
Facsimile: (212) 868-1229

*Attorneys for Plaintiff*